Introduction to Analysis – MA 542 – Fall 2019 – R. Pollack
HW #7 Solutions

Section 31:
1) Answer: $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$ with basis $\{1,\sqrt{2}\}$.

To justify this first note that $\sqrt{2}$ is a zero of x^2-2. To see that x^2-2 is the minimum polynomial of $\sqrt{2}$ over $\mathbb{Q}$ we need to know that it is irreducible. This can be seen in a number of different ways:

- prove that $\pm\sqrt{2}\notin\mathbb{Q}$ and thus this polynomial has no roots in $\mathbb{Q}$. Since the polynomial is quadratic this implies that it is irreducible;
- use the rational root theorem to deduce that this polynomial has no roots in $\mathbb{Q}$ and again deduce that it is irreducible;
- use the Eisenstein criterion with $p=2$.

Once we know that x^2-2 is the minimum polynomial of $\sqrt{2}$ we then immediately see that $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$ with basis $\{1,\sqrt{2}\}$ by the general fact:

Fact 1: $[F(\alpha):F]=n=\deg(\alpha,F)$ with basis $\{1,\alpha,\dots,\alpha^{n-1}\}$.

2) Answer: $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=4$ with basis $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$.

To justify this we first note that from #1 we know that $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$ with basis $\{1,\sqrt{2}\}$. We will now check that $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]=2$ with basis $\{1,\sqrt{3}\}$. This justifies our answer using the general fact:

Fact 2: $[L:F]=[L:K]\cdot[K:F]$ and L/F has basis $\{\alpha_i\beta_j\}$ if L/K has basis $\{\alpha_i\}$ and K/F has basis $\{\beta_i\}$.

To verify $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]=2$, we need to compute the minimum polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$. Clearly $\sqrt{3}$ satisfies x^2-3 so we need to check that this polynomial is irreducible over $\mathbb{Q}(\sqrt{2})$. To this end, assume it has a root in $\mathbb{Q}(\sqrt{2})$ so that there is some $a,b\in\mathbb{Q}$ such that $(a+b\sqrt{2})^2=3$. Then $a^2+2b^2+2ab\sqrt{2}=3$. We then deduce that $a^2+2b^2=3$ and $2ab=0$. (This deduction uses the fact that $\{1,\sqrt{2}\}$ is a basis of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$!). Thus $a=0$ or $b=0$. If $a=0$ then $2b^2=3$ with $b\in\mathbb{Q}$. Thus $2x^2-3$ has a root in $\mathbb{Q}$ which is impossible as this polynomial is Eisenstein with $p=3$. Now if $b=0$ then $a^2=3$ which leads to similar contradiction as x^2-3 is irreducible over $\mathbb{Q}$. Thus, no such $a+b\sqrt{2}$ can exist and we deduce that x^2-3 is irreducible over $\mathbb{Q}(\sqrt{2})$ proving our claim.

4) Answer: $[\mathbb{Q}(\sqrt[3]{2},\sqrt{3}):\mathbb{Q}]=6$ with basis $\{1,\sqrt[3]{2},\sqrt[3]{4},\sqrt{3},\sqrt{3}\sqrt[3]{2},\sqrt{3}\sqrt[3]{4}\}$.

To justify this we can proceed as before, but this situation is actually a bit simpler because the degree of $\sqrt[3]{2}$ and $\sqrt{3}$ are relatively prime. Namely, first note that $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$ with basis $\{1,\sqrt[3]{2},\sqrt[3]{4}\}$. Indeed, the minimum polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is x^3-2 as $\sqrt[3]{2}$ satisfies this polynomial and this polynomial is irreducible as it is an Eisenstein polynomial ($p=2$).

We now need to check that $[\mathbb{Q}(\sqrt[3]{2},\sqrt{3}):\mathbb{Q}(\sqrt[3]{2})]=2$ with basis $\{1,\sqrt{3}\}$. To this end, first note that $\sqrt{3}$ satisfies x^2-3 and so $\deg(\sqrt{3},\mathbb{Q}(\sqrt[3]{2}))$ is either 2 (if this polynomial is irreducible over $\mathbb{Q}(\sqrt[3]{2})$) or 1 (if $\sqrt{3}\in\mathbb{Q}(\sqrt[3]{2})$). So we need to rule out that $\sqrt{3}\in\mathbb{Q}(\sqrt[3]{2})$. But this is easy! If $\sqrt{3}\in\mathbb{Q}(\sqrt[3]{2})$ then $\mathbb{Q}(\sqrt{3})$ is a subfield of $\mathbb{Q}(\sqrt[3]{2})$ which implies that $[\mathbb{Q}(\sqrt{3}):\mathbb{Q}]$ divides $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]$. But then 2 divides 3 which is impossible! Thus $[\mathbb{Q}(\sqrt[3]{2},\sqrt{3}):\mathbb{Q}(\sqrt[3]{2})]=2$ with basis $\{1,\sqrt{3}\}$ (from fact 1).

Applying fact 2 with $L=\mathbb{Q}(\sqrt[3]{2},\sqrt{3})$, $K=\mathbb{Q}(\sqrt[3]{2})$ and $F=\mathbb{Q}$ then completes the question.

6) Answer: $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]=4$ with basis $\{1,\alpha,\alpha^2,\alpha^3\}$ with $\alpha=\sqrt{2}+\sqrt{3}$.

Solution 1: To see this, we compute the minimum polynomial of $\alpha = \sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$. To this end, note that

$$\alpha^2 = 2 + 3 + 2\sqrt{6}$$

and thus

$$(\alpha^2 - 5)^2 = (2\sqrt{6})^2 = 24.$$

Thus

$$\alpha^4 - 10\alpha^2 + 1 = 0$$

and α satisfies $x^4 - 10x^2 + 1$. We must now show that this polynomial is irreducible to deduce that it is the minimum polynomial.

To this end, note that it is not Eisenstein and that it is not irreducible modulo 2,3 or 5. So we need another method. First note that the polynomial has no roots in $\mathbb{Q}$ (by the rational roots theorem as 1 and -1 are not roots). We now need to rule out the case where this 4th degree polynomial factors as the product of two quadratics. Assume that it does so that

$$x^4 - 10x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (b + ac + d)x^2 + (ad + bc)x + bd$$

with $a, b, c, d \in \mathbb{Z}$. (We can assume these coefficients are in $\mathbb{Z}$ by Theorem 23.11.). Equating coefficients then gives that $bd = 1$, $b + ac + d = -10$ and $a + c = 0$. Since $bd = 1$ we deduce that $b = d = 1$ or $b = d = -1$. If $b = d = 1$, then $b + ac + d = -10$ becomes $ac = -12$. Since $a + c = 0$ we have $a = -c$ and then $ac = -12$ is equivalent to $a^2 = 12$ which is not solvable in $\mathbb{Z}$. Similarly, if $b = d = -1$, then $ac = -8$ which implies $a^2 = 8$ which again has no solutions. Thus $x^4 - 10x^2 + 1$ is irreducible over $\mathbb{Q}$ which justifies our answer by fact 1.

Solution 2: Note that

$$\frac{2 - 3}{\sqrt{2} + \sqrt{3}} = \sqrt{2} - \sqrt{3}.$$

Since $2 - 3$ and $\sqrt{2} + \sqrt{3}$ are in $\mathbb{Q}(\sqrt{2} + \sqrt{3})$, we deduce that $\sqrt{2} - \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. But then

$$\sqrt{2} + \sqrt{3} + \sqrt{2} - \sqrt{3} = 2\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

and

$$\sqrt{2} + \sqrt{3} - (\sqrt{2} - \sqrt{3}) = 2\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

Hence $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ and $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Since it is clear that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \supseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$, we deduce that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. By #2, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ and thus $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$.

8) Answer: $[\mathbb{Q}(\sqrt[3]{5}, \sqrt{2}) : \mathbb{Q}] = 6$ with basis $\{1, \sqrt[3]{5}, \sqrt[3]{25}, \sqrt{2}, \sqrt{2}\sqrt[3]{5}, \sqrt{2}\sqrt[3]{25}\}$.

The justification of this fact is nearly verbatim the justification of #4.

12) Answer: $[\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}(\sqrt{2} + \sqrt{3})] = 1$ with basis $\{1\}$.

By question #2, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. By question #6, $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$. Since $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ we deduce from fact 2 that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2} + \sqrt{3})] = 1$.

19)

a. False. Take $E = F = \mathbb{Q}$.

b. True.

c. False.

d. True (use fact 2 repeatedly)

23) Let α be any element of E which is not in F. Then $F(\alpha)$ is a subfield of E. Thus by Fact 2, $[E : F] = [E : F(\alpha)] \cdot [F(\alpha) : F]$. In particular, $[F(\alpha) : F]$ divides $[E : F]$. Since we are assuming that $[E : F]$ is prime, we deduce that $[F(\alpha) : F] = [E : F]$ or $[F(\alpha) : F] = 1$. But in the latter case, this implies that $F(\alpha) = F$ and hence $\alpha \in F$ which we assumed not to be the case. Thus $[E : F] = [F(\alpha) : F]$ which implies $[E : F(\alpha)] = 1$ and hence $E = F(\alpha)$ as desired.

27) **Solution 1 (hard way)**: We first check that $\mathbb{Q}(\sqrt{3}, \sqrt{7})$ has degree 4 over $\mathbb{Q}$. To do this we proceed in two steps by checking that

- $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$,
- $[\mathbb{Q}(\sqrt{3}, \sqrt{7}) : \mathbb{Q}(\sqrt{3})] = 2$.

The first equality is clear as the minimum polynomial of $\sqrt{3}$ over $\mathbb{Q}$ is $x^2 - 3$ (as in the solution to #1).

For the second equality, note that $\mathbb{Q}(\sqrt{3}, \sqrt{7}) = \mathbb{Q}(\sqrt{3})(\sqrt{7})$ and thus we need to determine the minimum polynomial of $\sqrt{7}$ over $\mathbb{Q}(\sqrt{3})$. To do this, note that $\sqrt{7}$ satisfies $x^2 - 7$ and so we must check that this polynomial is irreducible over $\mathbb{Q}(\sqrt{3})$. We do this by checking that it has no roots in $\mathbb{Q}(\sqrt{3})$.

To this end, assume that there exists $a, b \in \mathbb{Q}$ such that $(a + b\sqrt{3})^2 = 7$. Thus $(a^2 + 3b^2) + 2ab\sqrt{3} = 7$. Since $\{1, \sqrt{3}\}$ is a basis of $\mathbb{Q}(\sqrt{3})$ over $\mathbb{Q}$, we deduce that $a^2 + 3b^2 = 7$ and $2ab = 0$. Thus $a = 0$ or $b = 0$. If $b = 0$ then $a^2 = 7$. If $a = 0$ then $3b^2 = 7$. However, both polynomials $x^2 - 7$ and $3x^2 - 7$ are irreducible over $\mathbb{Q}$ as they are Eisenstein polynomials with $p = 7$. (Many other arguments are possible here: rational roots theorem, checking directly that $\sqrt{7} \notin \mathbb{Q}$, ...). This contradiction implies that $x^2 - 7$ has no roots in $\mathbb{Q}(\sqrt{3})$ and is thus irreducible over $\mathbb{Q}(\sqrt{3})$. Therefore $[\mathbb{Q}(\sqrt{3}, \sqrt{7}) : \mathbb{Q}(\sqrt{3})] = 2$

Now, by Fact 2,

$$[\mathbb{Q}(\sqrt{3}, \sqrt{7}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt{7}) : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

We now check that $\mathbb{Q}(\sqrt{3} + \sqrt{7})$ has degree 4 over $\mathbb{Q}$. To do this, we compute the minimal polynomial of $\alpha = \sqrt{3} + \sqrt{7}$ over $\mathbb{Q}$. We have

$$\alpha^2 = 3 + 7 + 2\sqrt{21}$$

and thus

$$(\alpha^2 - 10)^2 = (2\sqrt{21})^2 = 84.$$

Hence

$$\alpha^4 - 20\alpha^2 + 16 = 0$$

and α satisfies $x^4 - 20x^2 + 16$. To see this polynomial is irreducible over $\mathbb{Q}$, first note that it has no rational roots (as $\pm 16, \pm 8, \pm 4, \pm 2, \pm 1$ are not roots). Assume that there is a factorization

$$x^4 - 20x^2 + 16 = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (b + ac + d)x^2 + (ad + bc)x + bd$$

with $a, b, c, d \in \mathbb{Z}$. (We can assume these coefficients are in $\mathbb{Z}$ by Theorem 23.11.). Equating coefficients then gives that $bd = 1$, $b + ac + d = -20$ and $a + c = 0$. Since $bd = 16$ we deduce that (b, d) is one of $\{(1, 16), (2, 8), (4, 4), (-1, -16), (-2, -8), (-4, -4)\}$. Since $a = -c$, we have that $b + ac + d = -20$ is equivalent to $a^2 = 20 + b + d$. Running through the possible values of (b, d), we then see that a^2 must be one of the values $\{37, 30, 28, 12, 10, 3\}$. However, none of these values are a square in $\mathbb{Z}$. Thus $x^4 - 20x^2 + 16$ is irreducible over $\mathbb{Q}$ and is thus the minimum polynomial of $\sqrt{(3)} + \sqrt{7}$. Hence $\mathbb{Q}(\sqrt{3} + \sqrt{7})$ has degree 4 over $\mathbb{Q}$.

Finally, since $\mathbb{Q}(\sqrt{3} + \sqrt{7}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{7})$ we must have that these two fields are the same as they both have the same degree over $\mathbb{Q}$.

Solution 2 (easier way): Note that

$$\frac{3-7}{\sqrt{3}+\sqrt{7}} = \sqrt{3}-\sqrt{7}.$$

Since $3-7$ and $\sqrt{3}+\sqrt{7}$ are in $\mathbb{Q}(\sqrt{3}+\sqrt{7})$, we deduce that $\sqrt{3}-\sqrt{7} \in \mathbb{Q}(\sqrt{3}+\sqrt{7})$. But then adding and subtracting these two elements gives:

$$\sqrt{3}+\sqrt{7}+\sqrt{3}-\sqrt{7} = 2\sqrt{3} \in \mathbb{Q}(\sqrt{3}+\sqrt{7})$$

and

$$\sqrt{3}+\sqrt{7}-(\sqrt{3}-\sqrt{7}) = 2\sqrt{7} \in \mathbb{Q}(\sqrt{3}+\sqrt{7}).$$

Dividing by 2 gives $\sqrt{3}, \sqrt{7} \in \mathbb{Q}(\sqrt{3}+\sqrt{7})$ and hence $\mathbb{Q}(\sqrt{3},\sqrt{7}) \subseteq \mathbb{Q}(\sqrt{3}+\sqrt{7})$. Since it is clear that $\mathbb{Q}(\sqrt{3},\sqrt{7}) \supseteq \mathbb{Q}(\sqrt{3}+\sqrt{7})$, we deduce that $\mathbb{Q}(\sqrt{3},\sqrt{7}) = \mathbb{Q}(\sqrt{3}+\sqrt{7})$ as desired.

29) Assume that $p(x)$ has a zero α in E. Since $p(x)$ is irreducible, it must be the minimal polynomial of α over F. Thus $[F(\alpha):F] = \deg(p(x))$. However, by Fact 2, $[F(\alpha):F]$ divides $[E:F]$. But this is a contradiction as it was assumed that the degree of $p(x)$ does not divide $[E:F]$.